



HEALTH AFFAIRS



HIPAA Security Essentials

HIPAA Training: 2005 Summer Sessions

TMA Privacy Office

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Agenda

- Laws and Regulations
- Key Concepts and Terms
- DoD Security Regulation
 - General Information
 - Administrative Safeguards
 - Physical Safeguards
 - Technical Safeguards
- Introduction to Compliance

Training Objectives

- Upon completion of this lesson you will be able to describe:
 - Existing information security federal laws and regulations
 - Security and HIPAA terms and concepts
 - The Draft DoD Health Information Security Regulation requirements

Laws and Regulations

Laws and Regulations

Objectives



- After completing this module, you should be able to:
 - Identify the federal regulatory aspects of information security including laws and guidance
 - Describe the purpose and applicability of the HIPAA Security Rule

Legislative Requirements

- Federal laws and regulations require agencies to be accountable for results and provide security for information and assets
 - Health Insurance Portability and Accountability Act (HIPAA) of 1996
 - Office of Management and Budget (OMB) Circular A-123
 - Computer Security Act of 1987
 - OMB Circular A-130, Appendix III
 - Federal Information Security Management Act (FISMA)
 - Federal Managers Financial Integrity Act of 1982 (FMFIA)
 - Government Performance and Results Act (GPRA)

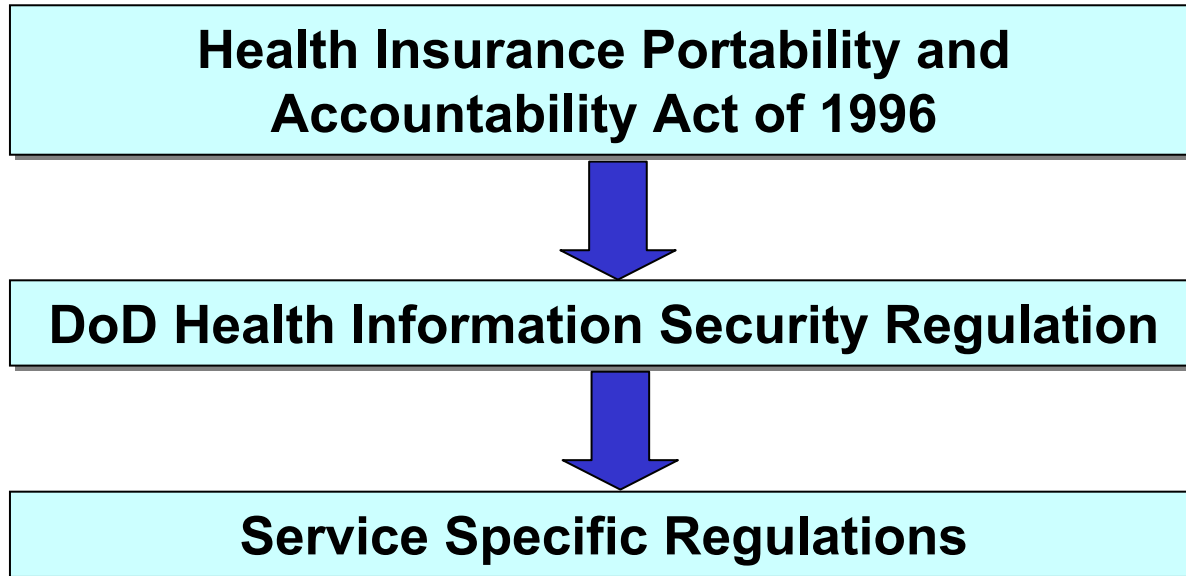
DoD Requirements (1 of 2)

- DoD regulations require agencies to be accountable for results, and provide security for information and assets
 - DoD 5000.1-D, Defense Acquisitions
 - DoD 5000.2-R, Mandatory Procedures for MDAS & MAIS Acquisition
 - DoD 5160.54-D, Critical Asset Assurance Program
 - DoD 5200.2-D, Personnel Security Program
 - DoD 5200.2-R, Personnel Security Program
 - DoD 5200.40-I, DITSCAP
 - DoD 5200.8-D, Security of DoD Installations & Resources
 - DoD 5200.8-R, Physical Security Program
 - DoD 5215.2-I, Computer Security Technical Vulnerabilities Reporting Program
 - DoD 6025.18-R, DoD Health Information Privacy
 - DoD 8000.1-D, Defense Information Management Program

DoD Requirements (2 of 2)

- DoD regulations continued
 - DoD 8000.1-D, Defense Information Management Program
 - DoD 8500.1-D, Information Assurance
 - DoD 8500.2-I, Information Assurance Implementation
 - DoD 8510.1-M, DITSCAP
 - DoD 8570.1-D, Information Assurance Training, Certification, and Workforce Management
 - DoD 8580.X-D, Security of Individually Identifiable Health Information in DoD Health Care Programs (Draft)
 - DoD 8580.X-R, DoD Health Information Security Regulation (Draft)
- Service-specific regulations

It Flows Downhill



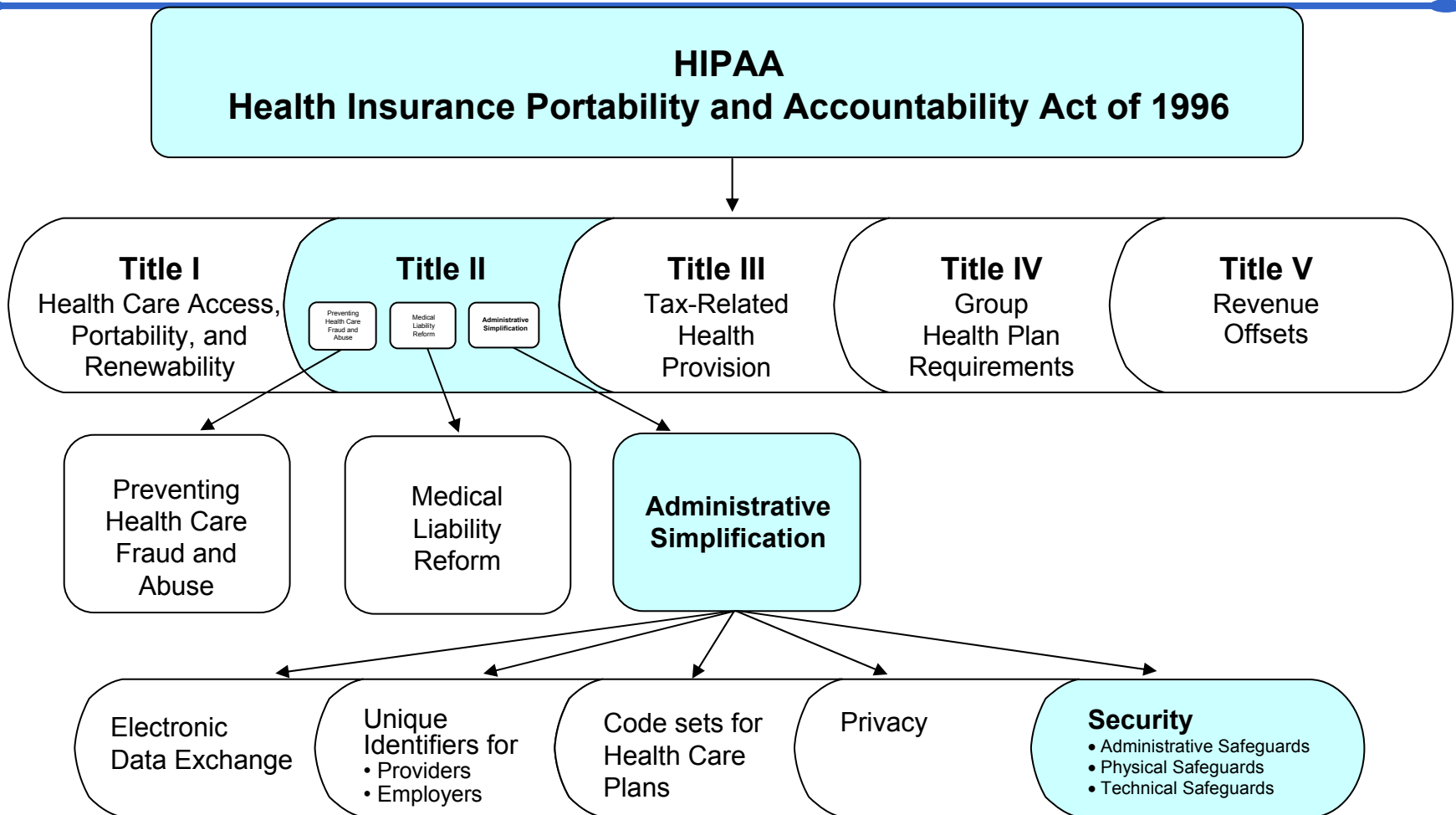
Laws and Regulations

HIPAA

- Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191
- Purpose
 - To adopt national standards for safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI)
 - Improves portability and continuity of health insurance coverage
 - Improves access to long term care services and coverage
 - Simplifies the administration of health care
 - Enacted August 21, 1996

Laws and Regulations





Where Does This Fit In?



Source: National Institute of Standards and Technology (NIST)

Laws and Regulations

Applicability of the HIPAA Security Rule

<u>HIPAA ENTITY</u>		<u>MHS ENTITY</u>
Providers who use a covered transaction		MTFs, DTFs, and clinics
Health plans		TRICARE Health Plan
Healthcare clearinghouses		Companies that perform electronic billing on behalf of MTFs
Business associates		Managed care support contractors and other contractors

Who is affected by HIPAA

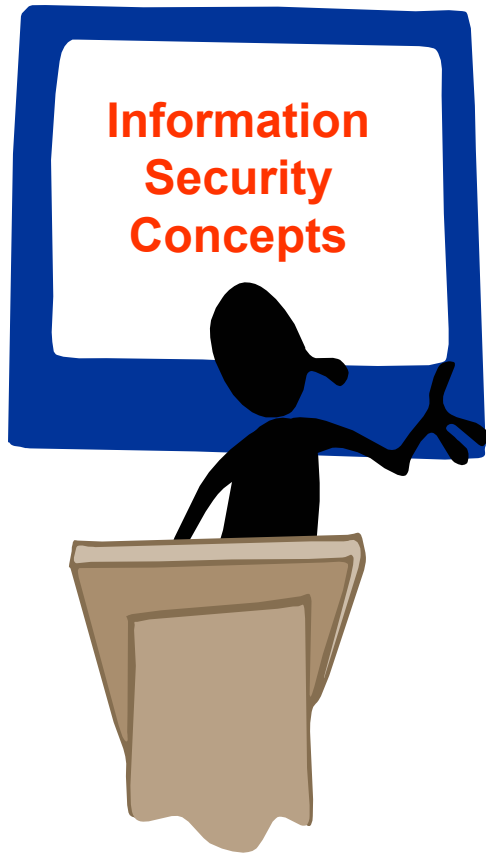
- All covered entities including:
 - MTFs
 - DTFs
 - Intermediate commands (HSOs, Regional Commands, etc)
 - Service Medical Department Headquarters
 - TMA
 - Operational units
 - Reserve forces when activated

Where is the HIPAA Security Rule Applicable?

- Anywhere the workforce is active
 - MTFs
 - Home
 - Field
 - On travel

Laws and Regulations

Summary



- You should now be able to:
 - Identify the federal and DoD regulatory aspects of information security including laws and guidance
 - Describe the purpose and applicability of the HIPAA Security Rule

Key Concepts and Terms

Key Concepts and Terms

Objectives

- Upon completion of this module, you should be able to:
 - Identify key concepts and terms pertaining to security, the DoD Security Regulation, and its requirements
 - Explain the differences between HIPAA Privacy and HIPAA Security
 - Identify examples of PHI and ePHI

Information Security

Information security is achieved through an integrated system of policies, procedures, products, and people that identify, control, and protect information from unauthorized disclosure and by an information protection strategy that is authorized by management and integral to good business practice.

Security Goals (1 of 2)

- **Confidentiality** – the property that data or information is not made available or disclosed to unauthorized persons or processes
- **Availability** – the property that data or information is accessible and useable upon demand by an authorized person



Security Goals (2 of 2)

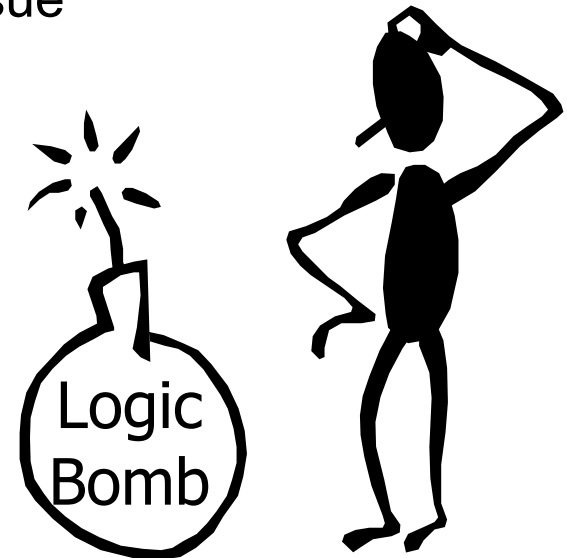
- **Integrity** – the property that data or information have not been altered or destroyed in an unauthorized manner



Key Concepts and Terms

Threat

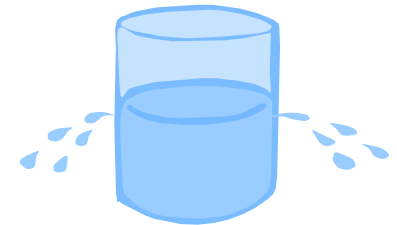
- A threat is the potential to cause unauthorized disclosure, changes, or destruction of an asset
 - Unauthorized disclosure = breach of confidentiality
 - Unauthorized changes = integrity failure
 - Unauthorized destruction = availability issue
- Types of threats:
 - Natural
 - Manmade
 - Environmental



Key Concepts and Terms

Threat Types

- Natural
 - Floods
 - Earthquakes
 - Tornadoes
 - Electrical Storms
- Manmade
 - Disgruntled employee
 - Arson
 - Social Engineering
 - Unintentional alterations
- Environmental
 - Long-term power failure
 - Pollution
 - Chemicals
 - Liquid Leakage



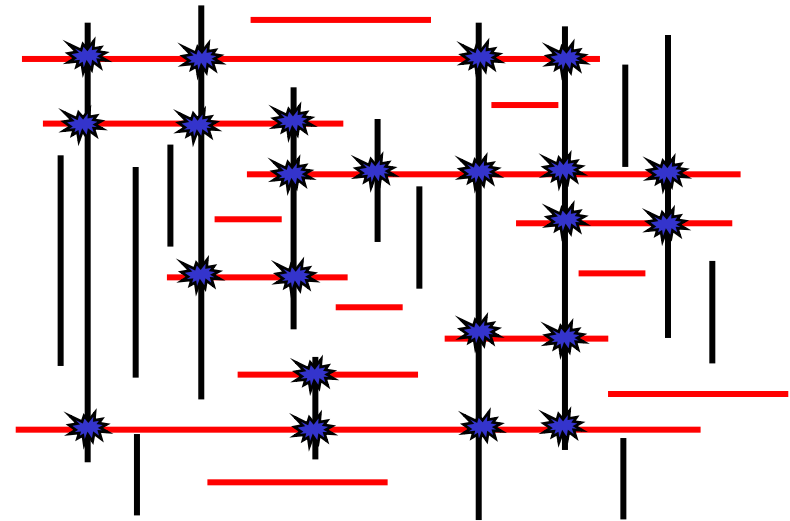
Vulnerability

- Any weakness in an information system, system security procedures, internal controls, or implementation that can be exploited
- Types of vulnerabilities:
 - Poorly communicated or implemented policy
 - Poorly trained personnel
 - Misconfigured systems or controls
 - Lack of access controls
 - Lack of physical controls
 - Lack of visitor policy

Key Concepts and Terms

What is Risk?

- A function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization



Key:



Threats



Vulnerabilities



Risks

Components of Risk



Security Incident

- The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system
- Including, but not limited to
 - Policy violations
 - Violations by users
 - Denial of service attacks
 - Intrusions
 - Unauthorized disclosures

Key Concepts and Terms

Safeguards

- Administrative
 - Administrative actions, policies and procedures, to manage the selection, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the organization's workforce in relation to the protection of that information
- Physical
 - Physical measures, policies, and procedures to protect an organization's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion
- Technical
 - Technology, policies, and procedures for its use that protect ePHI and control access to it

Key Concepts and Terms

HIPAA Key Terms

- Standards
- Implementation Specifications
- Required
- Addressable
- PHI / ePHI
- Compliance

Key Concepts and Terms

Standards

- HIPAA Security Rule contains standards and implementation specifications
 - Standards are requirements
 - Three categories of standards or safeguards:
 - Administrative
 - Physical
 - Technical
 - Standards state what to do, but not how to do it
 - Most standards have implementation specifications

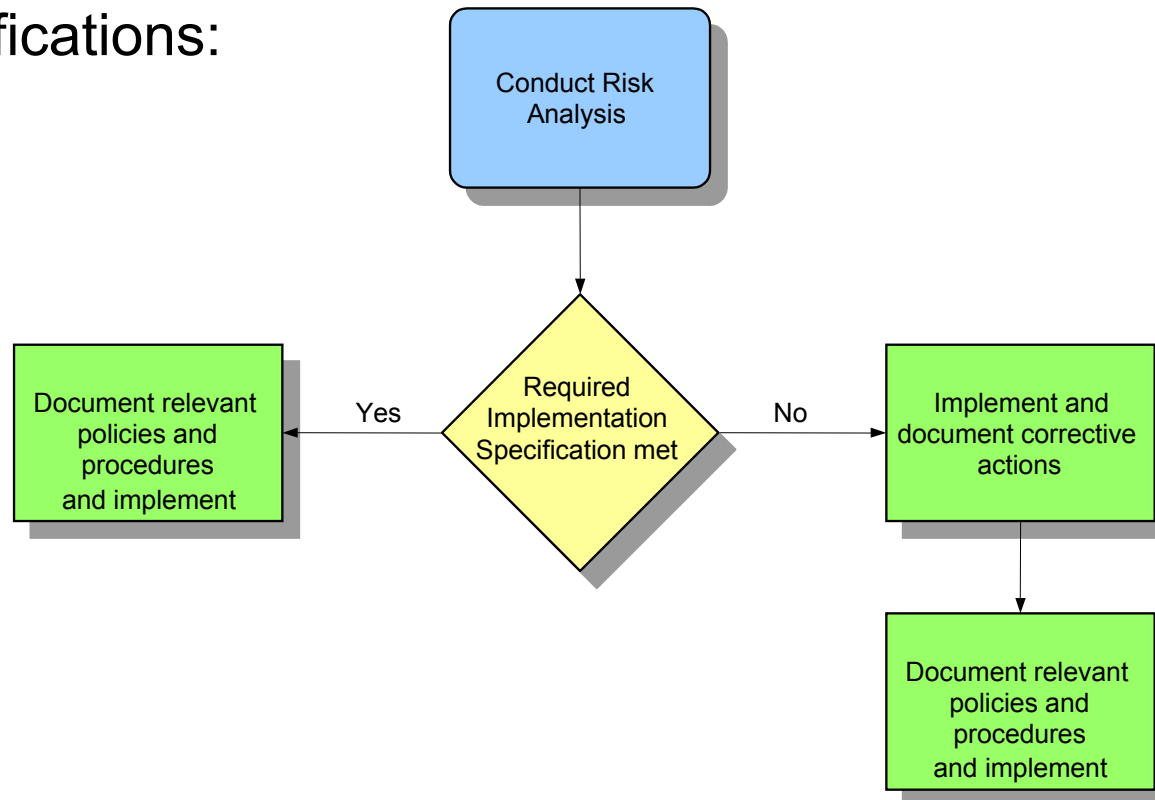
Implementation Specifications

- Implementation specifications support specific standards
- Provide instructions to assist meeting the standards
- Meeting all the implementation specifications does not automatically equate to meeting the standard
- In some cases, a standard itself provides sufficient information for implementation, in which case there is not a distinct implementation specification
- May be “required” or “addressable”

Key Concepts and Terms

Required

- **Required** means that covered entities must carry out the implementation specification at their facility
- For compliance with required implementation specifications:



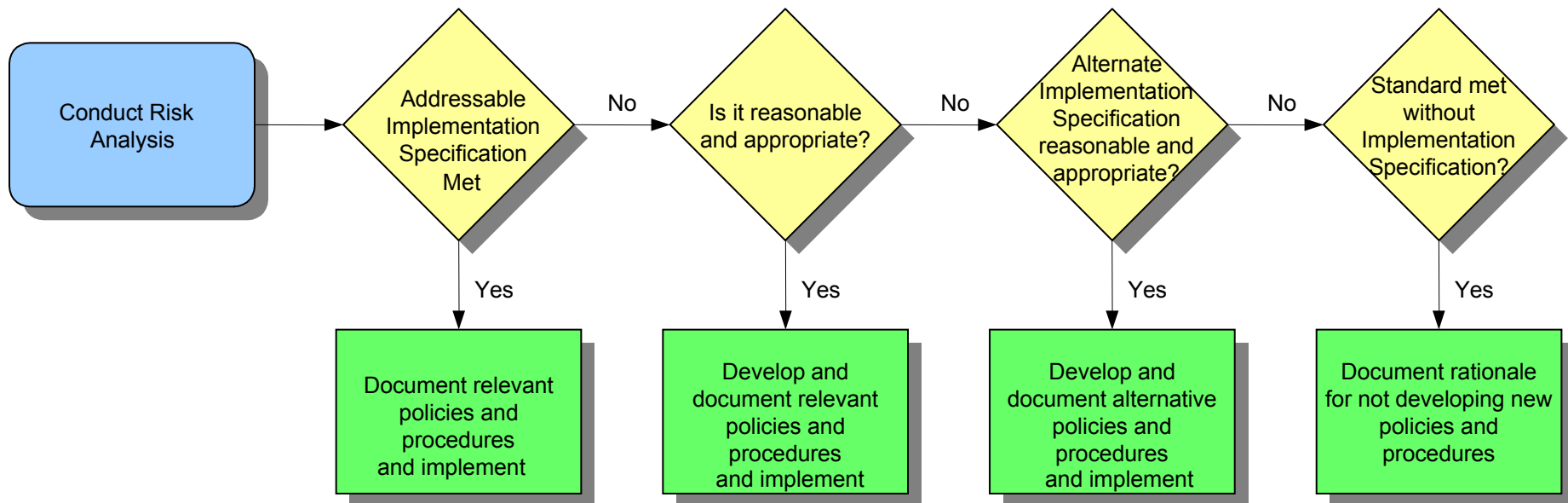
Addressable (1 of 2)

- **Addressable** means that covered entities must carry out the implementation specification if it is reasonable and appropriate
- For DoD, only three implementation specifications are addressable

Key Concepts and Terms

Addressable (2 of 2)

- For compliance with addressable implementation specifications:



Key Concepts and Terms

PHI / ePHI

- PHI is a sub-set of health information collected from an individual that is created or received by a health provider, health plan, or employer that meets certain criteria
- ePHI is PHI in electronic form that is transmitted or maintained by electronic media
- Not ePHI
 - Traditional fax, voice over telephone, paper copies

Key Concepts and Terms

PHI / ePHI – Criteria

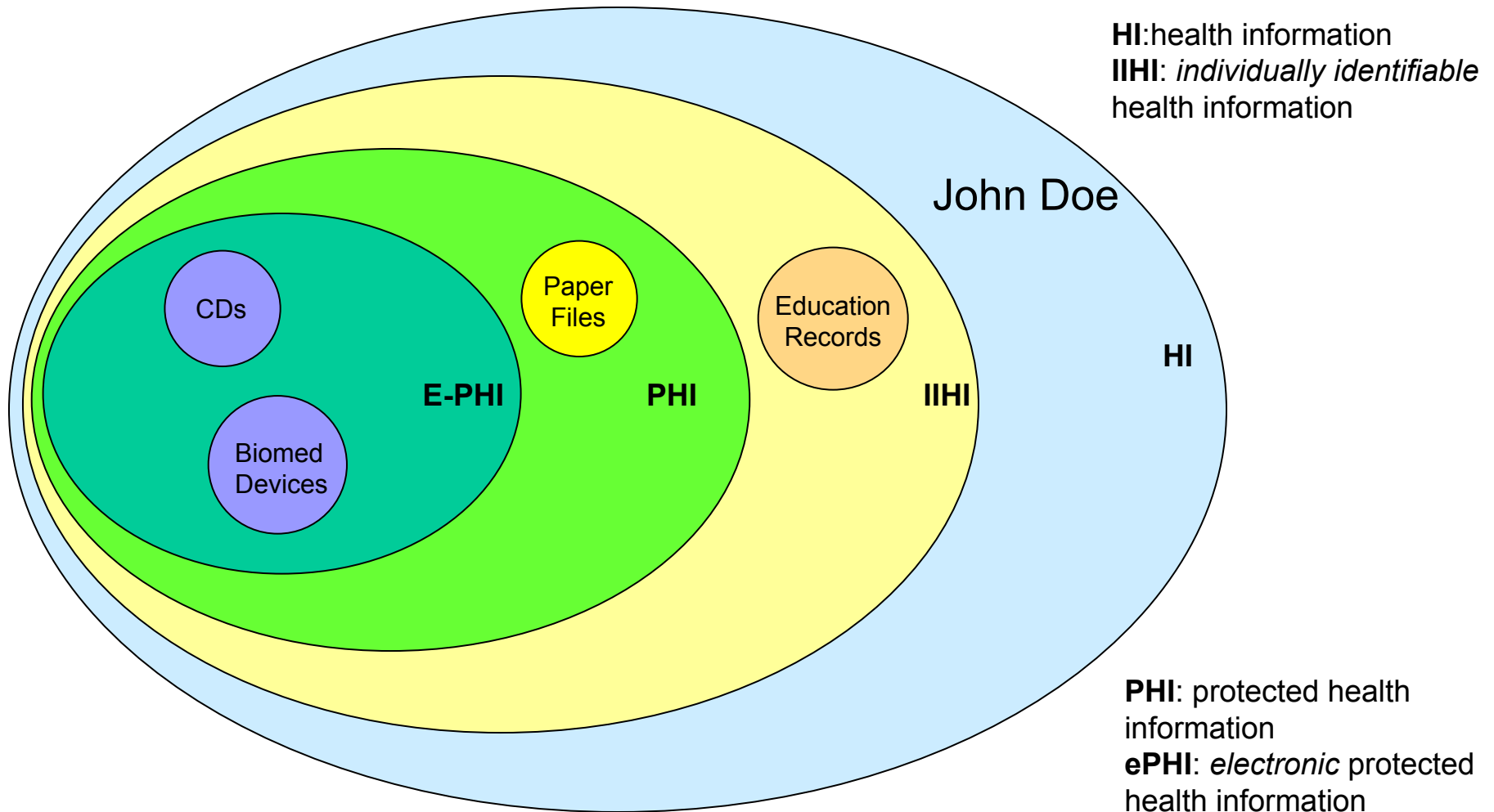
1. Includes past, present, and future information such as:
 - Demographics
 - Health
 - Payment for health services
2. Includes information that can be used to identify the individual

Note: Individually identifiable health information in employment or school records is not PHI



Key Concepts and Terms

The Universe of Health Information



Privacy vs Security

Privacy

- HIPAA 1996
- Covered entities
- April 14, 2003
- PHI
- Uses and Disclosures
- Confidentiality
- OCR

Security

- HIPAA 1996
- Covered entities
- April 20, 2005
- ePHI
- Safeguards
- Confidentiality, Integrity, and Availability
- CMS

Key Concepts and Terms

Compliance

- The Center for Medicare and Medicaid Services (CMS) approach toward HIPAA Security compliance:
 - Complaint driven
 - Voluntary compliance
 - Technical assistance
 - Corrective action plan
 - Progressive steps

Key Concepts and Terms

PHI / ePHI Activity (1 of 2)

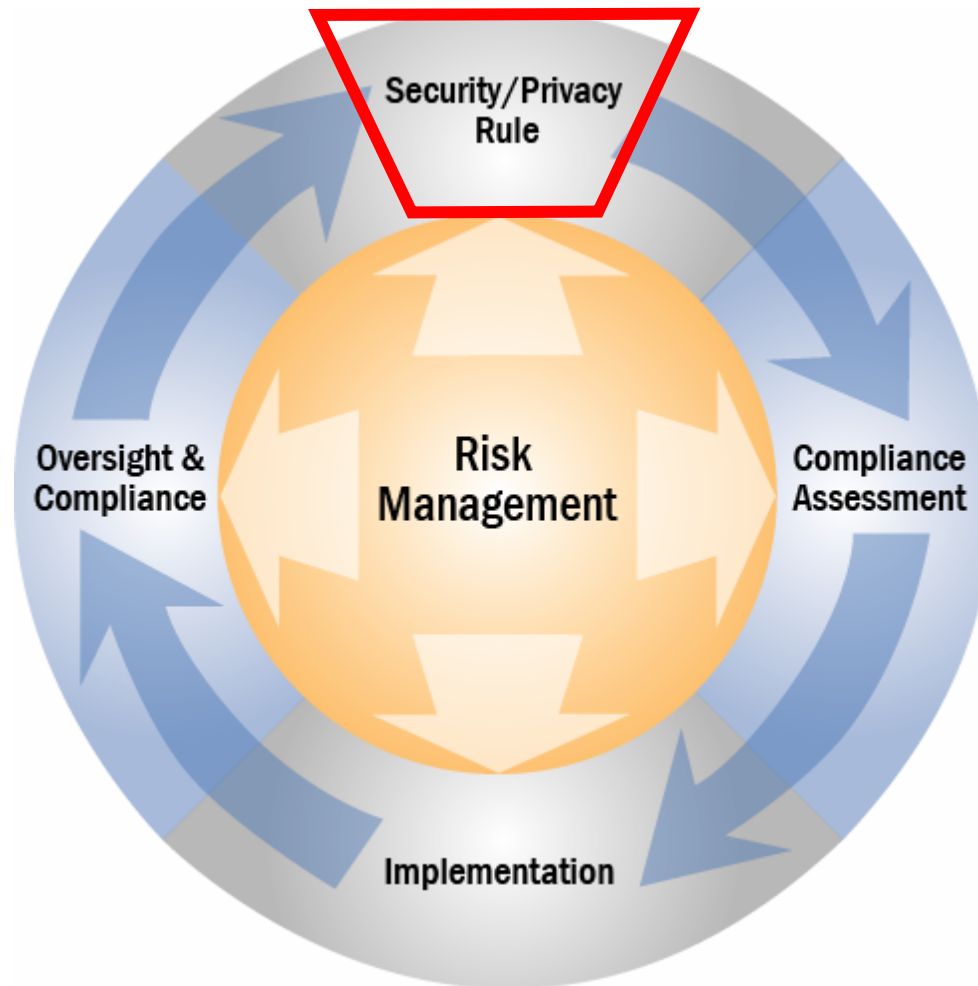
Activity	PHI	ePHI	Neither
Fax print out of a patient referral for an appointment	X		
Your medical history on your PDA			X
School immunization records			X
Digital phone message of appointment reminder		X	
Printed receipt for payment of medical services	X		
Diagnosis contained on MRI		X	
Printed patient medical history	X		

Key Concepts and Terms

PHI / ePHI Activity (2 of 2)

Activity	PHI	ePHI	Neither
Electronic college transcript			X
Lab results discussed over the telephone with a doctor	X		
Social Security Number			X
Pathology results saved to CD		X	
Username and password			X
A patient's name and health status emailed by family			X
Employee dental billing information on a laptop		X	

HIPAA Implementation Life Cycle



DoD Security Regulation

DoD Security Regulation

Objectives

- Upon completion of this module, you should be able to identify:
 - The organization of the DoD Security Regulation
 - Administrative, physical, and technical requirements (safeguards)
 - Identify the standards and implementation specifications that apply to the DoD
 - Describe which implementation specifications are addressable and which are required by DoD

General Information (1 of 4)

- **General Information**
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

General Information (2 of 4)

- Applicability
- Non-Applicability
- Policy
- Roles and Responsibilities

General Information (3 of 4)

- Applicability of the Regulation
 - The health plans of the MHS
 - Healthcare providers who transmit any health information in electronic form
- Non-Applicability
 - Drug testing program
 - Healthcare to foreign national beneficiaries of DoD when care is provided in a country other than the U.S
 - Armed Forces Repository of Specimen Samples for the Identification of Remains
 - Healthcare provided to enemy prisoners of war, retained personnel, civilian internees and other detainees

General Information (4 of 4)

- Non-Applicability continued
 - Education records maintained by domestic or overseas schools operated by DoD
 - Records maintained by day care centers operated by DoD
 - Reserve component medical activities not practicing in an MTF
 - Reserve component practicing outside the authority of MTF's who do not engage in electronic transactions covered by the Regulation

General Information – Policy (1 of 2)

- An organization must:
 - Ensure the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information
 - Protect against any reasonably anticipated uses or disclosures of information that are not permitted or required
 - Ensure compliance with the Regulation by its workforce
 - Assess whether addressable safeguards are reasonable and appropriate

General Information – Policy (2 of 2)

- Maintain the policies and procedures implemented to comply with this regulation in written (which may be electronic) form; and if an action, activity or assessment is required by this regulation to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment
 - Time limit: retain applicable documentation of policies, procedures, actions, activities, assessments for 6 years
 - Availability: make documentation available to involved persons
 - Updates: review documentation at a minimum annually and update as needed

General Information – Responsibilities (1 of 5)

- Specific responsibilities are delineated for:
 - Assistant Secretary of Defense for Health Affairs
 - Heads of DoD components
 - Security Officer
 - Designated Approving Authority
 - Program Manager
 - Information Assurance Manager
 - Information Assurance Officer
 - Privileged Users (SysAdmins, Network Security Officers)
 - Users

General Information – Responsibilities (2 of 5)

- Security Officer
 - Responsible for the development, implementation, maintenance, oversight, and reporting of security requirements for ePHI
 - Provide strategic and tactical program direction, and exercise authority over all programmatic components as necessary to accomplish ePHI security compliance
 - Ensure that requirements for ePHI are integrated into all policies and procedures for the planning, development, implementation, and management of the DoD infrastructure and information systems

General Information – Responsibilities (3 of 5)

- Security Officer continued
 - Perform internal audits of data access and use to detect and deter breaches of ePHI. Ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct
 - Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct involving PHI by evaluating or recommending the initiation of investigative procedures
 - Ensure consistent action is taken for failure to comply with ePHI security policies for all employees on the workforce. Work in cooperation with human resources, administration, and legal counsel, as appropriate

General Information – Responsibilities (4 of 5)

- Security Officer continued
 - Receive and document reports of security breaches relating to ePHI, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action
 - Complete job-specific training related to the protection of ePHI on an annual basis

General Information – Responsibilities (5 of 5)

- Other individuals who are part of the compliance initiative (but not specifically mentioned in the Security Regulation) include:
 - Privacy Officer
 - Physical Security Officer
 - Information Security Manager/Officer
 - MTF Analysis and Implementation Team (MISRT)
 - Incident response team
 - Any others as appropriate

Administrative Safeguards (1 of 3)

- General Information
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Administrative Safeguards (2 of 3)

- Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures through initial and subsequent organizational risk assessments due to changes in organizational security posture
- These measures are designed to protect ePHI and to manage the conduct of the organization's workforce in relation to the protection of that information

Administrative Safeguards (3 of 3)

- C2.2 Security Management Process
- C2.3 Assigned Security Responsibility
- C2.4 Workforce Security
- C2.5 Information Access Management
- C2.6 Security Awareness and Training
- C2.7 Security Incident Procedures
- C2.8 Contingency Plan
- C2.9 Evaluation
- C2.10 Business Associate Contracts and Other Arrangements

C2.2 Security Management Process

- Implement a security management process, including policies and procedures, to prevent, detect, contain, and correct security violations
- Specific Requirements:
 - Risk analysis
 - Risk management
 - Sanction policy
 - Information system activity review

C2.3 Assigned Security Responsibility

- Identify and assign in writing the security official for the organization who is responsible for the development and implementation of the policies and procedures required by the Security Regulation



C2.4 Workforce Security

- Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI and to prevent those workforce members who do not have authorized access from obtaining contact with ePHI
- Specific requirements:
 - Authorization and/or supervision
 - Workforce clearance procedures
 - Termination procedures

C2.5 Information Access Management

- Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements
- Specific requirements:
 - Access authorization
 - Access establishment and modification

C2.6 Security Awareness and Training

- Develop and implement a security awareness and training program for all members of the workforce that compliments the requirements of DoDD 8570.1
- Specific requirements:
 - Security reminders
 - Protection from malicious software
 - Log-in monitoring
 - Password management



C2.7 Security Incident Procedures

- Implement policies and procedures to address security incidents
- Specific requirements:
 - Response and reporting



C2.8 Contingency Plan

- Establish and review, annually, policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, and natural disaster that damages systems that contain ePHI
- Specific requirements:
 - Data backup plan
 - Disaster recovery plan
 - Emergency mode operation plan
 - Testing and revision procedures
 - Applications and data criticality analysis

C2.9 Evaluation

- Perform an annual (at a minimum) technical and non-technical evaluation, based upon this regulation and in response to environmental or operational changes affecting the security of ePHI. Establish the extent to which the organization's security policies and procedures meet the requirements of this regulation

C2.10 Business Associate Contracts and Other Arrangements (1 of 2)

- Business associates are authorized to create, receive, maintain, or transmit ePHI on behalf of the organization provided that minimal assurances are presented to the organization that the business associate will appropriately safeguard the information on its behalf
- Satisfactory assurances must be documented through a written contract or other legal arrangement with the business associate
- The contract or other arrangement must meet the requirements of paragraph C2.10.2

C2.10 Business Associate Contracts and Other Arrangements (2 of 2)

- Specific requirements:
 - Implement safeguards that protect ePHI
 - Ensure that any agent to whom it provides ePHI agrees to protect it
 - Report to the covered entity any security incident of which it becomes aware
 - CE may terminate a BA that has violated contractual terms
 - If a business associate is required by law to perform a function or activity on behalf...
 - The covered entity may omit from its other arrangements authorization...

Administrative Safeguards Activity

- Design an awareness and training campaign:
 - Choose one administrative safeguard as the focus of the campaign
 - Design a message
 - Identify a target audience
 - Create a communication plan
 - Define the approval process
 - Identify time frames required (mini POA&M)
 - Identify resource requirements
 - Identify opportunities to integrate into existing programs

Physical Safeguards (1 of 3)

- General Information
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Physical Safeguards (2 of 3)

- Physical measures, policies, and procedures to protect a organization's information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion



Physical Safeguards (3 of 3)

- C3.2 Facility access controls
- C3.3 Workstation use
- C3.4 Workstation security
- C3.5 Device and media controls

C3.2 Facility Access Controls

- Implement policies and procedures to limit physical access to information systems or biomedical devices and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
- Specific requirements:
 - Contingency operations
 - Facility security plan
 - Access control and validation procedures
 - Maintenance records

C3.3 Workstation Use

- Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI

C3.4 Workstation Security

- Implement physical safeguards for all workstations that access ePHI. Ensure that workstation access is only granted to authorized users and prevent workstations access to unauthorized users



C3.5 Device and Media Controls

- Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility
- Specific requirements:
 - Disposal
 - Media re-use
 - Accountability
 - Data backup and storage

Technical Safeguards (1 of 3)

- General Information
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Technical Safeguards (2 of 3)

- Technical safeguards are the technology, as well as the policies and procedures for its use, that protect ePHI and control access to it. The technical safeguards are designed to protect ePHI being created, processed, stored, or transmitted



Technical Safeguards (3 of 3)

- C4.2 Access controls
- C4.3 Audit controls
- C4.4 Integrity
- C4.5 Person or entity authentication
- C4.6 Transmission security

C4.2 Access Control

- Implement technical policies and procedures for information systems and electronic devices containing ePHI that allow access only to those persons or software programs that have been granted access rights
- Specific requirements:
 - Unique user identification
 - Emergency access procedure
 - Automatic logoff (A)
 - Encryption and decryption (A)

C4.3 Audit Controls

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI

C4.4 Integrity

- Implement policies and procedures to protect ePHI from improper or unauthorized access, use, disclosure, modification, alteration or destruction
- While organizations assure data integrity through a combination of many controls including administrative, physical and technical, this standard required the deployment and use of technical policies and procedures to protect data integrity
- Specific requirement:
 - Mechanism to authenticate ePHI

C4.5 Person or Entity Authentication

- Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. Install and use technical procedures that verify the identification and authentication of human users and other machines that transfer or request information

C4.6 Transmission Security

- Implement technical security measures to guard against unauthorized access, use, disclosure, modification, alteration, or destruction to ePHI that is being transmitted over an electronic communications network. Access and install appropriate technical controls that mitigate threats to data security in transit over all types of networks, including but not limited to, wireless networks, the Internet, corporate intranets, dedicated lease lines, and dial-up connections
- Specific requirements:
 - Integrity controls
 - Encryption (A)

DoD Security Regulation Summary

- You should be able to identify:
 - The organization of the DoD Security Regulation
 - Administrative, physical, and technical requirements (safeguards)
 - Identify the standards and implementation specifications that apply to the DoD
 - Describe which implementation specifications are addressable and which are required by DoD

Introduction to Compliance

Introduction to Compliance

Objectives

- Upon completion of this module, you should be familiar with:
 - Components to maintaining compliance with HIPAA Security
 - Process
 - Methods
 - Tools
 - Assurance

Process – Risk Analysis

- Risk Analysis is the key to:
 - Understanding what must be protected
 - Identifying potential risks and vulnerabilities
 - Initiating Risk Management

Process – Risk Management

- Risk Management, which includes risk analysis, is the process of
 - Assessing risk
 - Mitigating risk
 - Monitoring risk
- Important: Risk Management is a continuing process – not a one time event

Process – Risk Management Relevance to HIPAA

- Risk analysis determines the following key components to establishing HIPAA Security compliance:
 - The security risks involved in your organization's operations
 - The degree of response to security risks
 - Whether the addressable implementation specifications are reasonable and appropriate
 - Security measures to apply within your particular security framework
- Your ability to assess your state of compliance is greatly improved with risk analysis and a process for managing the data

Introduction to Compliance

Methods

- Methods to assist in establishing and maintaining compliance include
 - Gap / Compliance Assessment
 - Review of each requirement to ensure safeguards and documentation are in place
 - Missing or inadequate safeguards addressed in the risk management process
 - Risk Assessment / Management
 - Assessment of the threats and vulnerabilities relating to ePHI within the organization
 - Process of effectively mitigating risks found either in the risk assessment or through other means
 - Reporting
 - Monthly, quarterly and annual reporting to ensure management awareness and facilitate effective oversight

Introduction to Compliance Tools

- Tools include those provided by TMA
 - HIPAA BASICS™ Compliance Tool
 - HIPAA Training Tool (LMS)
 - OCTAVESM

Introduction to Compliance Assurance

- Compliance is established and maintained by implementing business practices including:
 - Measuring success
 - Identifying areas of improvement
 - Preparations and contingencies
 - Communication

Introduction to Compliance

Summary

- You should now be familiar with:
 - Components to establishing and maintaining compliance with HIPAA Security
 - Process
 - Methods
 - Tools
 - Assurance

HIPAA Security Essentials

Summary

- You should now be able to describe:
 - Existing information security federal laws and regulations
 - Security and HIPAA terms and concepts
 - The Draft DoD Health Information Security Regulation requirements

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- DoD 8580.X-R, DoD Health Information Security Regulation (Draft)
- [www.tricare.osd.mil/tmaprivacy/HIPAA.cfm](http://www.tricare.osd mil/tmaprivacy/HIPAA.cfm)
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA Security Representatives



HEALTH AFFAIRS



Please fill out your critique

Thanks!

